The Front Burner
Cyber Security

The ACIO for Cyber Security

Issue No. 11
October 2009

Wireless Computing in Public – Is Your Data Secure?

Whether you are sitting at the coffee shop waiting for a friend or sitting in the airport waiting on a plane, nothing beats the convenience of an Internet-connected laptop! But where there's convenience, there should be concern. How confident can you be that your private information is secure? Is a hacker trying to gain access to your computer?

Many public wireless access points, sometimes known as "hot spots", are not configured to protect information sent between your computer and the Internet; therefore, it can be very easy for people sitting nearby to gain access to the data in transit. This means they may be able to read everything sent and received by your computer, including credit card numbers and passwords. Or those same malicious users could be trying other ways to hack your computer through your connection. Here are some basic ways that you can reduce your risk and protect your information when you are in public:

Turn off wireless when not needed

Working on a document that is saved on your computer? If the convenience of a wireless connection is not important, turn off the wireless network card to avoid the possibility of inadvertently allowing access to your computer. This simple step can significantly reduce the risk of bad things happening.

Make sure to connect to the right network

Verify with a trusted source that you have the correct name of the network, or Service Set ID (SSID), for the wireless access point. An attacker could set up a system to impersonate the real access point so that you unknowingly connect to the Internet through the attacker's system. After that, it's easy for the attacker to compromise your information such as credit card numbers, confidential business data, etc.

Disable File Sharing

Allowing your files and folders to be "shared" on the computer is great for collaborating with trusted people on trusted networks. But it can be dangerous when you are connected to public networks. Always disable file sharing when connecting to a public network.

Is Someone Watching You?

Don't look now, but is that guy behind you watching over your shoulder? Using your computer in public makes it very easy for others to "shoulder surf" and see what you're doing. Attackers don't need sophisticated cracking programs if they can simply read your screen and watch you type!

Encrypt Sensitive Data

Always make sure that sensitive information is sent encrypted. For example, connections to corporate and government networks frequently use a Virtual Private Network (VPN) that encrypts all of the traffic, sometimes using additional authentication mechanisms, which is a great way to keep data confidential. Other good examples include web sites that ask for a password, credit card, or other sensitive information. Typically these web sites use Secure Sockets Layer (SSL), which encrypts the data being sent back and forth between your browser and the web site. Those websites will have a small "lock" icon in the bottom right corner of the browser frame and an "s" in the Web address bar (for example, "https"). If you are using a DOE-issued laptop, it is a requirement to encrypt all sensitive data stored on the laptop.

Stick with it!

Is it time for a refill on your coffee? As tempting as it is to leave your laptop for just a moment, that is long enough for the nice person, with whom you were just talking, to walk away with your data or the entire laptop! NEVER leave your laptop unattended!

Mark Your Calendars!
2010 Cyber Security Training Conference

Planning has begun for the DOE 2010 Cyber Security Training Conference. Next year's training event will be held in Atlanta, Georgia, May 17-21, 2010. There will be a variety of training workshops, track presentations, and networking opportunities available throughout the week. If you are interested in submitting an abstract, watch for the *2010 Call for Presentations* that will be distributed in the near future. If you have any questions or comments concerning the 2010 Cyber Security Training Conference, please send a message to: **cybsectrn@hq.doe.gov**.

Takin' it to the Streets
Cyber Security Awareness Campaign

For a second year, DOE successfully hosted a unique kind of Cyber Security Awareness Campaign, called ***Takin' It to the Streets!*** This event was held at Forrestal in August and Germantown in September and focused on helping employees *Shape Up and Get Cyber Fit*.

Awareness material was provided addressing current cyber topics both at home and in the workplace, to include keeping kids safe online, protecting personal information on social networking sites, adequate virus protection, mobile device security, green computing, destruction/ recycling of computing equipment, protecting privacy information, cyber forensics, etc. All of these topics help DOE employees be aware of and understand cyber security issues.

In the spirit of *getting cyber fit*, the event was also featured information from FOHO/GOHO and the Employee Assistance Program. More than 300 DOE employees came out to learn valuable tips on Cyber Fitness for both home and work.

Another Great Success!
2009 Cyber Security Awareness Day
October 22, 2009

Thank you to all of you who attended the 2nd Annual Cyber Security Awareness Day event and those of you who took the challenge and tested your Internet survival skills. As anticipated, DOE has some extremely 'cyber fit' employees fully equipped to tackle the Internet jungle! We certainly appreciate the feedback that our staff received – your feedback is critical as it aids with developing awareness programs and materials that meet our general users' needs.

This year's theme, ***Internet Survivor – Being Cyber Fit in the 21st Century***, highlights the real challenges and threats that we all face as Internet users. The purpose of this event was to reinforce awareness and understanding of cyber security challenges and threats and to provide timely and useful information that enables DOE employees to stay 'cyber fit' on the Internet, whether at home or in the workplace. Presentations were offered by leading cyber security professionals that addressed social networking, fighting cybercrime, and being an Internet security-savvy user. In addition, we were honored to have the National Center for Missing and Exploited Children participate again and present an update to their extremely popular and informative NetSmartz workshop, *Internet Safety for Parents*. Promotional materials, handouts, and a vendor expo were provided that reinforced presentation topics as well as addressed industry-endorsed, best cyber security practices. Finally, local DOE subject matter experts were on hand to answer employee questions and concerns.

If you have any comments or suggestions regarding any of the OCIO cyber security awareness events, please send them to cybsectrn@hq.doe.gov. Please check future *Front Burner* publications for information on additional cyber security awareness activities.

Cyber Hero Answers Your Security Questions

Q: What is the policy on accessing social network sites for business purposes?

A: OCIO cautions users of the security risks sometimes introduced by the use of these sites. The virtual world can pose security threats. Even just viewing a page on some of these sites can cause your computer to become infected with a virus, so look for anything at all unusual about such a site when you visit it or anything unusual about your computer after you have browsed on the site. DOE cyber security protection is unable to protect against some of these threats.

While social networking sites can provide innovative benefits, it is important to remember that their use for DOE work provides another medium for representation of our professional images. The same standards and ethical conduct applicable to regular business activities should be applied to social networking sites used for official DOE activities.